UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/476,037	12/31/1999	RODNEY A. KORN	042390.P6098	7224

7590 09/12/2003

GREGORY D CALDWELL
BLAKELY SOKOLOFF TAYLOR & ZAFMAN L L P
12400 WILSHIRE BOULEVARD SEVENTH FLOOR
LOS ANGELES, CA 90025

EXAMINER	
LEE, GRACE C	
ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 09/12/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/476,037	KORN, RODNEY A.	
	Examiner	Art Unit	
	Grace C. Lee	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____ .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-26 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-26 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 1-6, 9-16, 18, 20-26 are rejected under 35 U.S.C. 102(e) as being anticipated by Atkinson et al. (US Patent 6,367,012 B1, 'Atkinson' hereinafter).

Regarding claim 1, Atkinson disclosed a method for creating a secure script, comprising:

a) generating a hashed value for at least one executable command in the script;

> FIG. 3 is a flow diagram representing a code certification or signing method for ensuring the authenticity and integrity of a computer program, code, or an executable file received over computer network, or any other computer network. (col 6, line 19-23)
>
> Process block indicates that a cryptographic digest or "hash" (FIG. 4) of executable file is obtained or computed. (col 6, line 39-41)

b) signing the hashed value to create a signed hashed value;

Process block indicates that a publisher signature (FIG. 4) is formed with cryptographic digest. (col 6, line 50-51)

c) appending the signed hashed value to the script.

publisher signature are attached or appended to or incorporated to executable file. (the last line of col 6 continue to the first line of col 7)

Regarding claim 2, the method of claim1, wherein generating a hashed value for at least one executable command in the script comprises providing the executable command as a key value that is input to a mathematical function, computing the mathematical function, and providing as output from the mathematical function the hashed value.

Atkinson disclosed (see col 6, line 44-50), these functions take a variable-length input string and convert it to a fixed-length output string of 128 bits or more (called a cryptographic digest). This fixed-length string "fingerprints" the file by producing a value that indicates whether a file submitted for download matches the original file. Hashing functions and the values they generate are secure in that it is computationally infeasible to alter a document without changing its hash.

Regarding claims 3-5, wherein signing the hashed value to create a signed hashed value comprises encrypting the hashed value; wherein encrypting the hashed value comprises encrypting the hashed value using a cryptographic key;

wherein encrypting the hashed value using a cryptographic key comprises encrypting the hashed value using a public encryption private key.

Atkinson disclosed (see col 6, line 55-56), publisher signature is formed with a public-private key signature algorithm.

Regarding claim 6, wherein the script is component in a World Wide Web document downloaded from a HyperText Transfer Protocol server to a client for execution thereon.

Atkinson disclosed that typical HTML documents found on the world wide web include both text and tags specifying files for several images that are to be displayed with the text. In use, browser software allows a user to navigate (also known as "browsing") between documents and sites on the world-wide web. (col 1, line 29-31). The files that browsers are capable of accessing and utilizing include executable files such as, for example OLE controls and JAVA applets. it is expected that the functionality of such executable files will increase to include a wide range of applications and application components. (col 1, line 36-43)

Atkinson also disclosed software recipient to obtain additional information before deciding to run downloaded code. (col 9, line 16-20)

Regarding claim 9, a method for securing a script, comprising: a) computing a hashed value for each executable command in a script; b) encrypting the hashed value for each executable command in the script; and c) appending to the script the encrypted hashed values for each executable command.

Claim 9 is rejected as per claim 1.

Regarding claim 10, wherein encrypting the hashed value for each executable command in the script comprises encrypting the hashed value for each executable command with a public encryption private key.

Claim 10 is rejected as per claim 5.

Regarding claims 11-12, further comprising signing a control program, comprising the script and a public key corresponding to the private key, to keep hidden the public key; wherein signing the control program comprises encrypting the control program using a second public encryption private key.

Atkinson disclosed (see col 7, line 6-8), publisher signature and publisher digital certificate together form a keyed source confirmation with a secure representation of the executable file. The source confirmation is keyed in that it (or a portion of it) is encrypted with a key, or includes a key, or both. A source confirmation with publisher signature and publisher digital certificate as described is both encrypted with a key and includes a key.

Regarding claims 13-15, wherein the control program is an ActiveX control in an application program; wherein the ActiveX control is in a HyperText Markup Language (HTML) document; wherein the HTML document is downloaded from a HyperText Transfer Protocol (HTTP) server to a HTTP client.

Atkinson disclosed (see Abstract), the executable file may be of any executable form, including an executable or portable executable .exe file format, a .cab cabinet file format, an .ocx object control format, or a Java class file.

Regarding claim 16, Atkinson disclosed a method for executing a script

a) computing a hashed value for each executable command in a script;

A cryptographic digest or hash is determined for the code as it is received. (col 3, line 18-19),

b) decrypting an encrypted hashed value appended to the script for each executable command in the script to obtain a decrypted hashed value for each executable command in the script;

The digest is compared to the digest included in the publisher signature. (col 3, line 19-20)

c) comparing the computed hashed value for each executable command in the script with the corresponding decrypted hashed value for each executable command in the script; and

The digest is compared to the digest included in the publisher signature. (col 3, line 19-20)

d) executing the executable commands in the script if the computed hashed values for the executable commands in the script are the same as the corresponding decrypted hashed values appended to the script for the executable commands.

A match between the digests confirms the integrity of the code. A dialog is then rendered by the recipient computer indicating who is providing the code and the certification agency that has authenticated the identity of the publisher (col 3, line 20-24). The dialog can be rendered by browser application, for example, and can include user queries as to whether to open or run executable file. (col 8, line 24-26)

Regarding claim 18, first comprising verifying a public key cryptography signature associated with a control program comprising the script.

Atkinson disclosed the publisher signature is decrypted with publisher's public key (col 8, line 27-28).

Regarding claim 20, wherein the script is in a HyperText Markup Language (HTML) document.

Claim 20 is rejected as per claim 14.

Regarding claim 21, wherein the HTML document is downloaded to a Hypertext Transfer Protocol (HTTP) client from a HTTP server.

Claim 21 is rejected as per claim 15.

Regarding claim 22, performed by an ActiveX control in the HTML document.

Claim 22 is rejected as per claim 13.

Regarding claims 23, which is a processor instructions claim as per claim 9.

Regarding claims 24, which is a processor instructions claim as per claim 16.

Regarding claims 25, which is an apparatus claim as per claim 9.

Regarding claims 26, which is an apparatus claim as per claim 16.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 7-8, 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Atkinson et al. (US Patent 6,367,012 B1, "Atkinson" hereinafter) in view of Ogilvie (US Patent 6,324,650 B1).

Regarding claims 7 and 8, Atkinson disclosed the signed hashed value appended to the script. Atkinson failed to teach encrypting the script with a symmetric encryption key. Ogilvie disclosed that the system may encrypt (or re-encrypt) the information during an optional encrypting step 312 to secure the sensitive information. The disclosure conditions, formats, and/or destinations may also be encrypted (col 10, line 57-59). Possible formats include plaintext, digitally signed, encrypted, XML or HTML, and other formats for electronic documents (col 10, line 19-21). Encryption tools and techniques are well-known in the art, and any suitable ones may be used, including without limitation public key-private key encryption, symmetric encryption, and/or encryptions described in Schneier, Applied Cryptography and other references (col 10, line 60-64). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to encrypt the script with a symmetric encryption key to secure the sensitive data.

Regarding claim 17, wherein the script is an encrypted script, further comprising decrypting the encrypted script with a symmetric encryption key to obtain the script.

Claim 17 is rejected per claims 7 and 8. The encrypted script using a symmetric encryption key has to be decrypted with a symmetric encryption key to obtain the script.

5. Claim 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over Atkinson et al. (US Patent 6,367,012 B1, "Atkinson" hereinafter) in view of McManis (US Patent 6,546,487 B1).

Regarding claim 19, Atkinson disclosed (a) computing a hashed value; (b) decrypting an encrypted hashed value appended to the script; (c) comparing the computed hashed value with decrypted hashed value. Atkinson failed to teach repeating computing (a) and comparing (c) to prevent dynamic modification. McManis disclosed a single digital signature for each program module, and the associated message digest is computed using a hash function (col 4, line 55-57). The digital signature must match corresponding message digest computed by the verifier in order the verifier to return a verification confirmation message, and then to execute the program procedure calls (col 4, line 66-67, continue to the first line of col 7, abstract). The Procedure A calls Procedure B, then Procedure B calls Procedure C, then Procedure C calls Procedure D ... (see Application Modules A, B, C, D ...in Fig 1), this is a repeating computing and comparing to complete executing a program. Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to repeat computing (a) and comparing (c) in order to complete executing a program/script. This repeating prevents dynamic modification to a program/script so that the integrity of a script in an application is accomplished.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Grace C. Lee whose telephone number is 703-305-0710. The examiner can normally be reached on Monday - Friday 8:00 am - 4:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 703-305-1830. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

GL

Grace C. Lee
Examiner
Art Unit 2132

GCL

GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100